DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Automating STIGs

Compliance and Enforcement

Brady Alleman
Senior Cyber Security Engineer
16 May 2019

What is STIG automation?

- **A Security Technical Implementation Guide provides:**
  - A set of security hardening requirements for a platform
  - Discussion and rationale for requirements
  - Manual procedures for evaluating the system (checks)
  - Manual procedures for implementing the requirement (fixes)
- **Automated implementations are derived from the STIG**
  - The STIG remains the authoritative requirements source
  - Official automated content is published in the SCAP format

What is SCAP?

- **Security Content Automation Protocol**
- **US Government Standard (NIST SP 800-126)**
- **Required for use in DoD by DoDI 8500.01**
- **Primarily used for automated assessments (checks) of STIG rules**
- **DISA publishes automated SCAP content for some STIGs**
- **Why are some items not automated?**
  - Limitations of the STIG procedure
  - Limitations of the SCAP standard
  - Limitations of DoD SCAP tools
- **Remediation**
  - Supports inclusion of “fix” content
  - Capability not required of products by the SCAP Validation Program

What about other tools?

- **For our purposes, Configuration Management (CM) tools:**
  - Enforce managed systems into approved configurations
  - Allow for declarative specification of configuration settings
  - Are intended for repeated application (e.g., idempotent)
- **Examples:**
  - PowerShell DSC
  - Chef
  - Ansible
  - Puppet

Goals for STIG content for CM tools

- **Leverage CM tools to enforce STIG requirements**
- **Allow for customization**
  - Enforcement of individual rules may be enabled or disabled
  - Setting values are configurable
  - Configuration is exposed using native CM tool capabilities
- **Use a STIG-centric approach**
  - Implement configurations to match STIG rules one-for-one when possible
  - Use STIG identifiers (STIG ID, Rule IDs) to allow for cross-reference
- **Use native or existing capabilities**
  - Native CM resource where available
  - Community-sourced or custom resources when needed

What have we implemented?

- **Windows Server 2016**
  - PowerShell DSC
  - Chef
- **Red Hat Enterprise Linux 7**
  - Chef
  - Ansible
- **Cisco IOS-XE**
  - Ansible
- **Tool selection based on initial survey of capabilities with preference given to solutions native to the platform**
- **Content available on forge.mil under the STIG Collaboration project**

There is no mandate; use this content if it helps you!

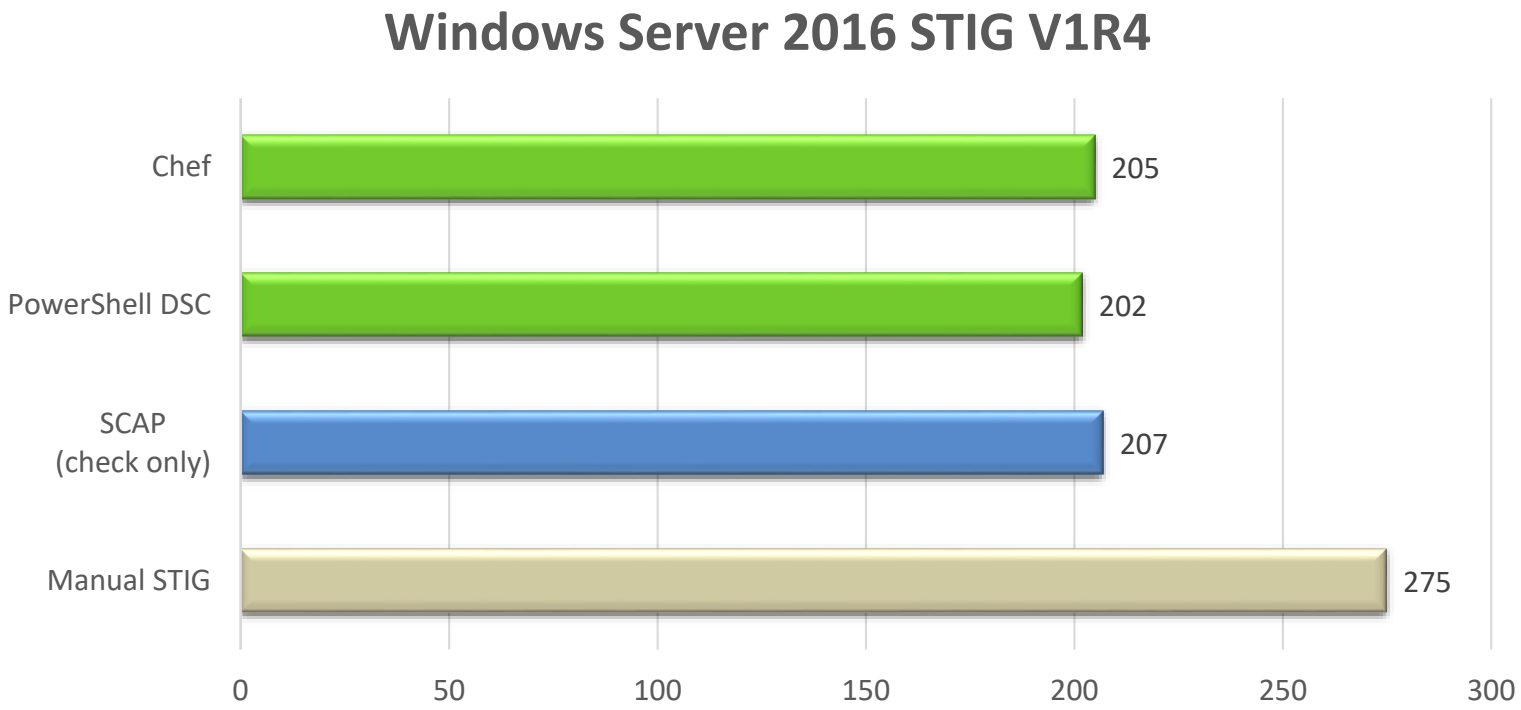
Windows Server 2016 – Use Cases

- **Group Policy remains a first choice**
  - Robust framework native to Windows domains
  - GPOs are already published on IASE
- **Potential uses for CM STIG content on Windows**
  - Nano Server (lacks Group Policy support)
  - Standalone systems
  - Environments preferring management using CM tools

Windows Server 2016 - Implementations

- **PowerShell DSC**
  - Native capability provided by Windows
  - Leverages Microsoft-provided modules
- **Chef**
  - Leverages Microsoft-provided PowerShell DSC modules
  - Can leverage Chef infrastructure for central control

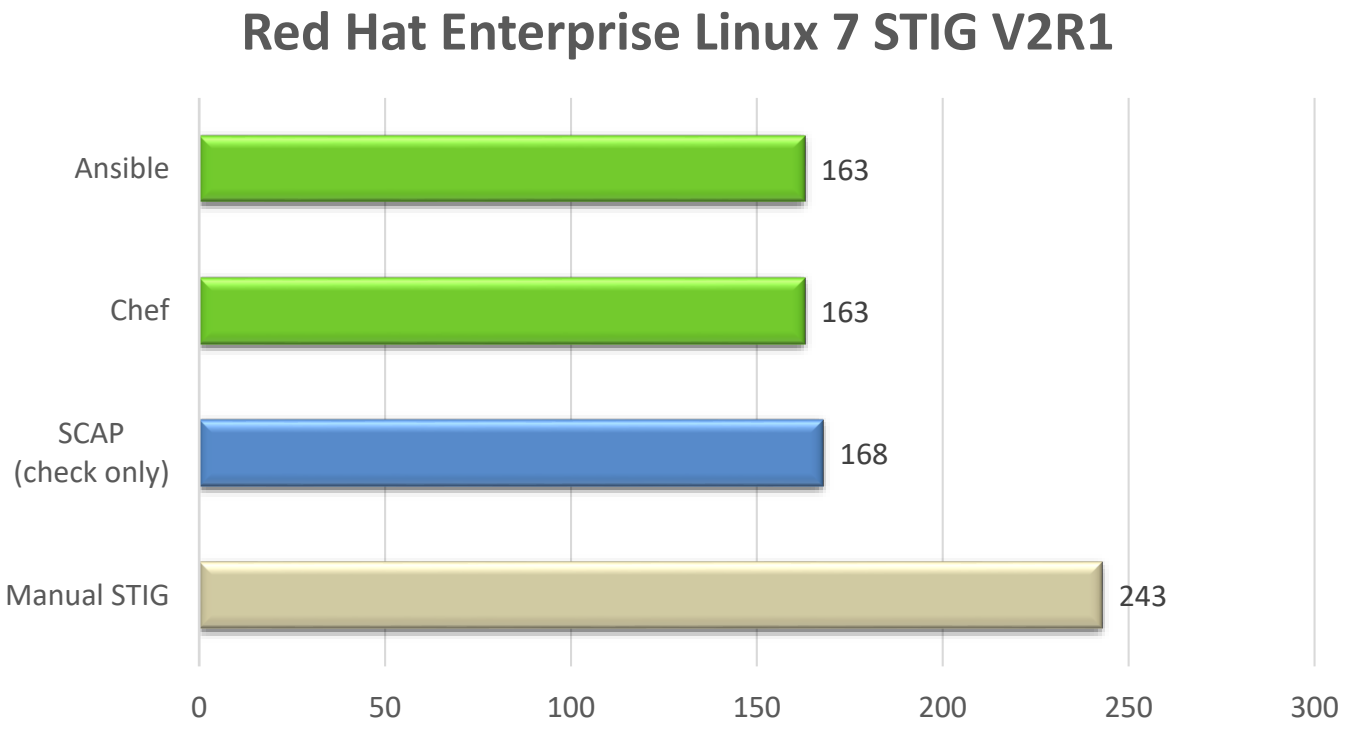
Windows Server 2016 - Coverage



Red Hat Enterprise Linux 7 - Implementations

- **Chef**
  - Uses 3rd party “puppet_compat” cookbook from the Chef Supermarket
- **Ansible**
  - Uses native Ansible resources
  - Recommend latest version (2.7)

Red Hat Enterprise Linux 7 - Coverage



Cisco IOS-XE Release 3 - Implementations

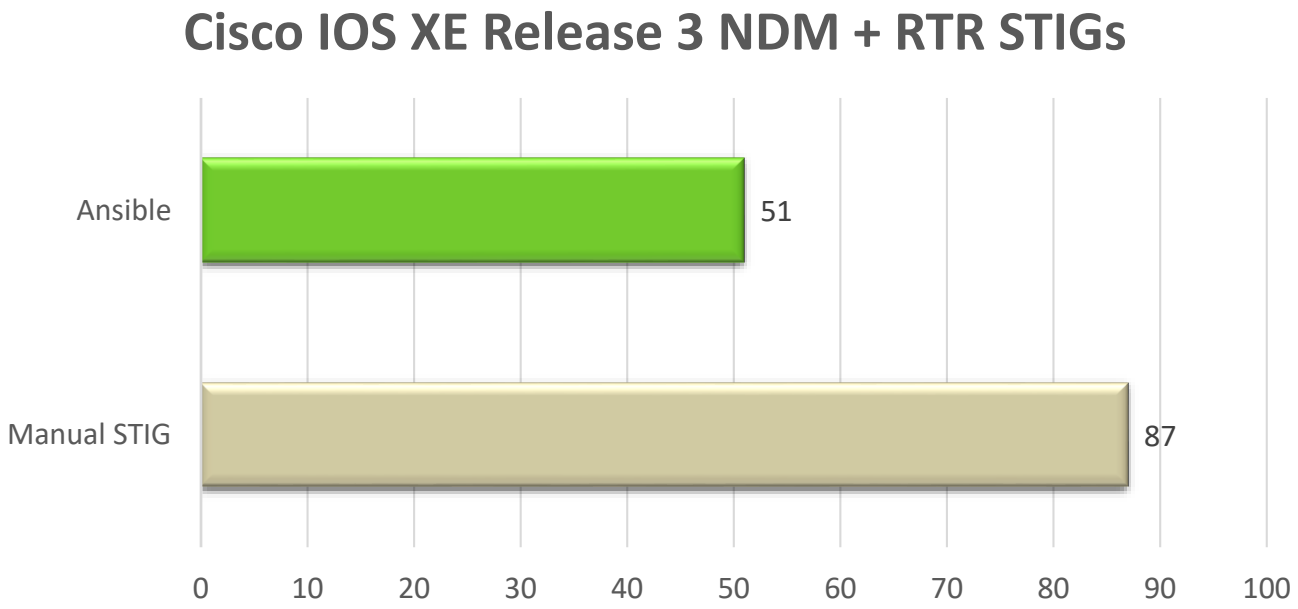
Covers two STIGs:

- Cisco IOS XE Release 3 NDM
- Cisco IOS XE Release 3 RTR

Ansible

- Recommend latest release (2.7)

Cisco IOS-XE Release 3 - Coverage



Future Work

- Maintenance updates to existing content
- Additional STIG and tool coverage
- Efforts will be influenced by STIG community feedback

Questions

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**

visit us

DISA Booth 1929

follow us

Facebook/USDISA

Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at **www.disa.mil/about/industry-partners**.